TIJ's RoLD Virtual Forum on Cybercrime
วันพฤหัสบดีที่ 18 มิถุนายน พ.ศ. 2563

Keynote address by
Mr. Jeremy Douglas, UNODC Regional Representative
ปาฐกถา โดย
นายเจเรมี ดักลาส ผู้แทนประจำภูมิภาคเอเชียตะวันออกเฉียงใต้และแปซิฟิก สำนักงานว่าด้วยยาเสพติด และอาชญากรรมแห่งสหประชาชาติ (UNODC)

Good Evening Ladies and Gentlemen.
สวัสดีแขกผู้มีเกียรติทุกท่าน

On behalf of the United Nations Office on Drugs and Crime, it is my pleasure to be a part of this virtual discussion of the Rule of Law and Development Programme initiated by the Thailand Institute of Justice. This is a very important opportunity for UNODC and our long standing partner the TIJ to have an open discussion about cybercrime, current trends, challenges faced, and how we contribute to building a resilient cyberspace in Thailand as well as the greater ASEAN region.

ในนามของสำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (UNODC) ผมรู้สึกยินดีเป็นอย่างยิ่งที่ได้เป็นส่วนหนึ่งในการอภิปรายออนไลน์ของโครงการด้านหลักนิติธรรมและการพัฒนา ที่ริเริ่มโดยสถาบันเพื่อความยุติธรรมแห่งประเทศไทย (TIJ) การอภิปรายในวันนี้ ถือเป็นโอกาสที่สำคัญอย่างยิ่งที่สำนักงาน UNODC และองค์กรพันธมิตรที่ยาวนานอย่าง TIJ จะได้ร่วมกันนำเสนอถึงแนวโน้มและความท้าทายของอาชญากรรมไซเบอร์ และความร่วมมือในการสร้างพื้นที่ออนไลน์ (cyberspace) ที่ปลอดภัยมั่นคงในประเทศไทย รวมถึงในภูมิภาคอาเซียน

Modern technology has transformed the way we communicate and live day-to-day and has shifted the economic and societal focus of

countries within Southeast Asia and the Pacific. With the advent of “Thailand 4.0”, the country aims to transform the economy by fostering and embracing creativity, research, and development through digitization. Such a digital transformation also requires the country to face major challenges including cybersecurity and cybercrime.

เทคโนโลยีสมัยใหม่ได้เปลี่ยนแปลงรูปแบบการสื่อสาร การดำเนินชีวิต และได้เปลี่ยนแปลงรูปแบบทางเศรษฐกิจและสังคมของประเทศในเอเชียตะวันออกเฉียงใต้และแปซิฟิก ด้วยวิสัยทัศน์ “ประเทศไทย 4.0” ประเทศไทยได้มุ่งเน้นให้เกิดการปฏิรูปทางเศรษฐกิจ โดยการส่งเสริมให้เกิดความคิดสร้างสรรค์ การวิจัยและการพัฒนา ผ่านกระบวนการใช้เทคโนโลยีดิจิทัล อย่างไรก็ดี การเปลี่ยนแปลงด้านเทคโนโลยีดิจิทัลนี้ ก็ส่งผลให้ประเทศไทยต้องเผชิญกับความท้าทายต่างๆ รวมถึงความท้าทายด้านความมั่นคงปลอดภัยทางไซเบอร์และอาชญากรรมไซเบอร์

The development of cyber space has also created new opportunities for criminals to exploit, launch a destabilizing threat, and or disrupt services associated with critical infrastructure of a nation. The risks associated with the misuse of cyber are also borderless, and often exacerbate traditional trans-border crimes such as drug smuggling, and human-trafficking, and there is a need for diplomacy. ASEAN will need to overcome intra-bloc differences operationally and strategically by fostering partnership among governments and private entities.

การพัฒนาของพื้นที่ออนไลน์เปิดโอกาสให้เกิดการก่ออาชาญากรรมในรูปแบบต่างๆ เพื่อการแสวงหาผลประโยชน์ สร้างภัยคุกคามต่อเสถียรภาพ และ/หรือ การทำลายบริการต่างๆ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานที่สำคัญของประเทศ อีกทั้งการใช้ไซเบอร์ในทางที่ผิดยังมีลักษณะไร้พรมแดนและทำให้อาชญากรรมข้ามพรมแดนแบบดั้งเดิม เช่น การลักลอบขนยาเสพติดและการค้ามนุษย์ทวีความรุนแรงมากขึ้น ความร่วมมือทางการทูตจึงเป็นสิ่งที่จำเป็นอย่างมาก อาเซียนจะต้องร่วมมือกันแก้ไขปัญหาเรื่องความแตกต่างภายในภูมิภาค ทั้งในเชิงปฏิบัติและเชิงกลยุทธ์ โดยเฉพาะการส่งเสริมความเป็นพันธมิตรระหว่างรัฐบาลและหน่วยงานเอกชน

Ladies and gentlemen,
ท่านผู้มีเกียรติทุกท่าน

The cyber threat landscape is transforming rapidly in Thailand and Southeast Asia. More and more **critical infrastructure** is being connected exposing it to the new threats. **Hackers** are constantly trying to access and steal data related to regional political, economic, and military issues with the design of sophisticated malware. The evolution of **malware** has contributed significantly to the development of what my cyber team refers to as an attack landscape. **Network based ransomware cryptoworms** are also on the rise, eliminating the human element in the launch of ransomware campaigns. A rise in the use of **unmonitored and unpatched IoT devices** have made companies more susceptible to **botnet attacks**. **Malicious e-mail scams, business email compromise and phishing** are still prominent in the region and remain one of the vital tools for criminals to disseminate malware along with social engineering techniques.

สถานการณ์ภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงอย่างรวดเร็วทั้งในประเทศไทยและในภูมิภาคเอเชียตะวันออกเฉียงใต้ ระบบโครงสร้างพื้นฐานสำคัญที่มีความเชื่อมโยงกันมากขึ้นจึงเสี่ยงต่อการถูกโจมตี อาชญากรไซเบอร์ หรือ แฮกเกอร์ มักพยายามเข้าถึงระบบและลักลอบขโมยข้อมูลสำคัญทางด้านการเมือง เศรษฐกิจ และทางการทหารของภูมิภาค ผ่านการใช้โปรแกรมประสงค์ร้ายหรือมัลแวร์ในรูปแบบต่างๆ ซึ่งวิวัฒนาการของมัลแวร์เหล่านี้มีความสำคัญอย่างยิ่งต่อการพัฒนาของสิ่งที่ทีมงานด้านอาชญากรรมไซเบอร์ของสำนักงาน UNODC เรียกว่า สถานการณ์การโจมตี (attack landscape) นอกจากนั้น การติดแรนซัมแวร์ หรือไวรัสเรียกค่าไถ่ ประเภทเวิร์มโดยใช้ข้อมูลเป็นตัวประกัน ก็มีเพิ่มมากขึ้น และกระจายตัวได้อย่างรวดเร็วด้วยเช่นกัน การใช้งานอุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตที่ล้าสมัยหรือไม่ได้ถูกติดตั้งระบบการรักษาความปลอดภัยที่ดีพอ ทำให้หลายองค์กรตกอยู่ในความเสี่ยงต่อการถูกโจมตีโดยเครือข่าย Botnet ที่ลักลอบเข้าควบคุมระบบและก่อความเสียหายสูงต่อระบบขององค์กร การหลอกลวงโดยใช้อีเมล โดยอ้างที่มาจากหลากหลายองค์กรหรือหน่วยงานสำคัญยังคงเป็นการภัยคุกคามที่สร้างความเสียหายในระดับประเทศและระดับ

ภูมิภาคตลอดมา และยังคงเป็นเทคนิคการหลอกลวงที่ใช้เป็นเครื่องมือในการแพร่กระจายมัลแวร์เพื่อการก่ออาชญากรรมในรูปแบบต่างๆ

With the rise of the Internet of Things (IoT) devices being used within the government and private infrastructure, **Distributed Denial of Service (DDoS)** attacks have increased in severity and scope. **Romance scams** also remain a prominent method of fraud using social media whereby victims are tricked into involvement into romantic situations, and then drawn to crime including fraud, or their blackmail. And o**nline Child Sexual Exploitation** is also on the rise within the region where predators watch abuse on live-streaming sites with a form of payment through pseudo-anonymous cryptocurrencies.

การใช้งานอุปกรณ์ที่สามารถเชื่อมต่อกับอินเทอร์เน็ตที่เพิ่มขึ้นในองค์กรภาครัฐและภาคเอกชนนั้น ทำให้การโจมตีแบบ Distributed Denial of Service หรือการโจมตีโดยปฏิเสธการให้บริการแบบกระจาย ได้มีโอกาสในการจู่โจมเป้าหมายและทวีความรุนแรงยิ่งขึ้น นอกจากนี้ การใช้เทคนิค Romance scam หรือการหลอกลวงโดยใช้ความเสน่หา ยังคงถูกนำมาใช้ในการหลอกลวงเหยื่อผ่านสื่อสังคมออนไลน์ จนนำไปสู่การเกิดอาชญากรรมในหลากหลายรูปแบบ อย่างเช่น การหลอกลวงและการแบล็คเมล ยิ่งไปกว่านั้น ปัญหาการแสวงหาประโยชน์ทางเพศจากเด็กบนสื่อออนไลน์ยังคงพบเห็นได้มากภายในภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยการเข้าไปดูการถ่ายทอดสดการละเมิดของเด็กทางสื่อออนไลน์ต่างๆ ผ่านการจ่ายเงิน โดยใช้สกุลเงินดิจิตัลแบบไม่ระบุตัวตน

Thankfully, over recent years, several websites containing child abuse materials have been taken down by Thai Authorities. UNODC commends this work and the proactive approach carried out by authorities to apprehend pedophiles.

ในหลายปีมานี้ ประเทศไทยเองก็ได้ดำเนินการเพื่อจัดการกับสื่อออนไลน์ที่ล่วงละเมิดทางเพศต่อเด็กให้หมดไป ซึ่งทางสำนักงาน UNODC รู้สึกชื่นชมในการทำงานและการใช้มาตรการเชิงรุกเพื่อจับกุมผู้ล่วงละเมิดเหล่านั้นด้วย

At the same time, the sudden boom in ICT has given rise and safe havens for transnational organized crime groups online through various **anonymous black marketplaces**. These groups are able to quickly adapt and exploit technology making it more complex and sophisticated for the criminal justice system to detect, deter and disrupt criminal activities online. Thailand is no exception.

ในขณะเดียวกัน การเติบโตอย่างรวดเร็วของเทคโนโลยีสารสนเทศก็กลายเป็นแหล่งพักพิง (safe haven) ในการประกอบกิจการผิดกฎหมายของอาชญากรรมข้ามชาติออนไลน์ ผ่านทางตลาดมืดที่ไม่เปิดเผยตัวตนต่างๆ (anonymous black marketplaces) ซึ่งกลุ่มอาชญากรเหล่านี้สามารถปรับตัวและใช้ประโยชน์จากเทคโนโลยีได้อย่างรวดเร็ว ทำให้เกิดความซับซ้อนสำหรับกระบวนการยุติธรรมทางอาญา ในการค้นหา ยับยั้ง และขัดขวางการก่ออาชญากรรมออนไลน์ ซึ่งประเทศไทยเองก็ไม่ใช่ข้อยกเว้น

The use of the Internet and more specifically its hidden side, the **“Darknet”**, for selling illegal commodities has increased substantially on a global level and Southeast Asia is also a victim in this regard. By exploiting anonymity provided by relay networks such as TOR, combined with other easy to learn and acquire obfuscation techniques, an individual can train and collaborate on crime, sell or buy almost any kind of illegal merchandise, and pay with virtually untraceable or pseudo anonymous cryptocurrencies.

การใช้อินเทอร์เน็ตโดยเฉพาะด้านที่ไม่เปิดเผย อย่าง “Darknet” หรือเครือข่ายอินเทอร์เน็ตที่ขายสินค้าผิดกฎหมายนั้นเติบโตขึ้นอย่างมากในระดับโลก และภูมิภาคเอเชียตะวันออกเฉียงใต้ก็ประสบปัญหานี้เช่นเดียวกัน การใช้ประโยชน์จากการไม่เปิดเผยตัวตนจากเครือข่ายแบบรีเลย์ (relay network) เช่น TOR (The Onion Router) หรือ บริการที่ทำให้คนสามารถท่องอินเทอร์เน็ตโดยไม่เปิดเผยตัวตน ร่วมกับเทคนิคอื่นๆ ทำให้อาชญากรสามารถฝึกฝนและทำงานร่วมกันเพื่อ

ก่ออาชญากรรม ทำการซื้อขายสินค้าผิดกฎหมายเกือบทุกประเภท และทำการชำระเงินเสมือนจริงที่ไม่สามารถแกะรอยได้ หรือ ใช้สกุลเงินดิจิทัลปลอม (pseudo anonymous cryptocurrencies)

Darknet entrepreneurs were quick to seize the opportunity to monetize the advantages of network anonymity and create hidden services that freely advertise illegal or controlled items over the Internet such as drugs, fake or counterfeited IDs/passports, firearms, cybercrime toolkits, child abuse material, protected or endangered wildlife products and so on. These activities have also proliferated a **crime-as-a-service** model where various types of criminals, from hitmen to hackers to scammers or kidnapers, offer their services on hidden services or platforms hosted on Darknets. Recent engagement of UNODC with member states highlights that countries within Southeast Asia have relatively low or disproportionate understanding and awareness of the cybercrime threats they are facing.

ผู้ประกอบการ Darknet ได้ใช้โอกาสในการสร้างรายได้อย่างรวดเร็วจากเครือข่ายที่ไม่เปิดเผยตัวตน และสร้างบริการแบบซ่อนที่มีการโฆษณาสินค้าแบบผิดกฎหมายหรือสินค้าควบคุม ผ่านทางอินเทอร์เน็ตอย่างเสรี เช่น ยาเสพติด หนังสือเดินทางหรือบัตรประจำตัวประชาชนปลอม อาวุธปืน ชุดเครื่องมือสำหรับอาชญากรรมทางไซเบอร์ สิ่งของสำหรับการล่วงละเมิดเด็ก สินค้าเกี่ยวกับสัตว์ป่าคุ้มครองหรือสัตว์ใกล้สูญพันธุ์ เป็นต้น กิจกรรมเหล่านี้ทำให้รูปแบบกิจกรรมแบบ crime-as-a-service เพิ่มจำนวนขึ้นอย่างรวดเร็ว ซึ่งมีอาชญากรหลายประเภทตั้งแต่มือปืนไปจนถึงผู้ที่ลักลอบเข้าระบบ ผู้ปลอมแปลงตัวตนเพื่อหลอกลวงผู้อื่นในโลกออนไลน์ หรือพวกลักพาตัว ซึ่งได้เสนอบริการของพวกเขาในบริการแบบซ่อน หรือแพลตฟอร์มบน Darknet ทั้งนี้ จากการทำงานของสำนักงาน UNODC กับรัฐสมาชิก ทำให้ว่าประเทศต่างๆ ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ยังขาดความเข้าใจและความตระหนักเกี่ยวกับการคุกคามทางไซเบอร์ที่พวกเขากำลังเผชิญอยู่

Ladies and gentlemen,
ท่านผู้มีเกียรติทุกท่าน

With several lockdown measures applied by governments across Southeast Asia and the Pacific due to COVID-19, social distancing has resulted in increased isolation of individuals, encouraging people to use the Internet for purchasing essential commodities needed for daily life.

มาตรการล็อคดาวน์ที่ได้ประกาศใช้โดยรัฐบาลทั่วภูมิภาคเอเชียตะวันออกเฉียงใต้และแปซิฟิก อันเนื่องมาจากสถานการณ์การแพร่ระบาดของ COVID-19 ส่งผลให้คนต้องอยู่แยกกันมากขึ้นเพื่อรักษาระยะห่างทางสังคม และส่งเสริมให้พวกเขาใช้อินเทอร์เน็ตในการซื้อสินค้าที่จำเป็นสำหรับชีวิตประจำวัน นอกจากนี้ มาตรการดังกล่าวก็ทำให้คนต้องทำงานจากที่บ้านและต้องพึงพาการใช้ช่องทางดิจิทัลต่างๆ ในการทำงานและใช้ชีวิต เด็กที่ต้องกักตัวอยู่บ้านก็มีการใช้สื่อสังคมออนไลน์ เล่นเกมส์ และเรียนออนไลน์มากขึ้น ผู้สูงอายุที่รู้สึกเหงาจากการกักตัวก็อาจจำเป็นต้องเพิ่มการใช้สื่อสังคมออนไลน์เพื่อติดต่อกับครอบครัวเช่นเดียวกัน

The fact is that cybercrime poses significant risks to economies worldwide. We have extensive experience countering cybercrime and will continue to provide technical assistance through long-term whole-of-government responses. We will also continue to closely cooperate with, guide and advise key partners to minimize duplication of effort, help deconflict assistance, and serve to aid the building of a comprehensive threat picture. Our engagement with ASEAN Member States to date has positioned us as a trusted partner for matters related to cybercrime issues and we are uniquely placed to provide support to Member States in both the short term and longer-term. A couple of highlights include;

อาชญากรรมไซเบอร์ส่งผลกระทบอย่างมีนัยสำคัญต่อเศรษฐกิจโลก โดยสำนักงาน UNODC มีประสบการณ์ในการจัดการกับปัญหาดังกล่าว และจะดำเนินการให้ความช่วยเหลือทางวิชาการแก่รัฐบาลทุกภาคส่วนต่อไปเพื่อให้การป้องกันและปราบปรามอาชญากรรมไซเบอร์เป็นไปในทิศทางเดียวกัน นอกจากนี้ เราจะสนับสนุน ให้คำแนะนำ และร่วมมืออย่างใกล้ชิดกับองค์กรพันธมิตร เพื่อลด

ความซับซ้อนในการทำงานและการให้ความช่วยเหลือ และช่วยทำให้ทุกฝ่ายสามารถมองเห็นภาพของภัยคุกคามไซเบอร์ในองค์รวมได้อย่างชัดเจน ในส่วนของความร่วมมือในระดับภูมิภาคนั้น สำนักงาน UNODC เป็นพันธมิตรสำคัญของประเทศสมาชิกอาเซียนในการให้ความช่วยเหลือด้านอาชญากรรมไซเบอร์ทั้งในระยะสั้นและระยะยาว ยกตัวอย่างเช่น

- We have been providing operational mentoring and capacity building training to criminal justice authorities to detect, identify, collect, and investigate criminal activities in the Darknet using Cryptocurrencies; Online Child Sexual Exploitation; and to use Cyberthreat Intelligence in counter-terrorism operations.
- We have helped establish the first Digital Forensics Laboratory in Lao PDR.
- We have also been developing a ***"Cyber Threat and Darknet Assessment"*** of ASEAN countries, obtaining necessary information from law enforcement, legal and policy counterparts to analyse capacity and the cyber landscape. UNODC will launch the report this year.

- ให้คำปรึกษาด้านปฏิบัติการและการฝึกอบรมเสริมสร้างศักยภาพแก่เจ้าหน้าที่ด้านความยุติธรรมทางอาญา ในการตรวจสอบ จำแนก รวบรวมหลักฐาน และสอบสวนการกระทำผิดทางอาญา ในการใช้ Cryptocurrency หรือ สกุลเงินดิจิตอล บน Darknet การแสวงหาประโยชน์ทางเพศจากเด็กในโลกออนไลน์ และการใช้ Cyberthreat Intelligence หรือ ระบบคลังข้อมูลภัยทางไซเบอร์อัจฉริยะ ในปฏิบัติการต่อต้านการก่อการร้าย
- จัดตั้งห้องปฏิบัติการด้านพิสูจน์พยานหลักฐานดิจิทัลแห่งแรกในประเทศลาว
- พัฒนาการประเมินภัยคุกคามทางไซเบอร์และดาร์กเน็ต โดยใช้ข้อมูลจากหน่วยงานบังคับใช้กฎหมาย หน่วยงานด้านกฎหมายและนโยบาย เพื่อวิเคราะห์ศักยภาพและสถานการณ์ด้านไซเบอร์ของประเทศในอาเซียน และมีกำหนดเผยแพร่รายงานดังกล่าวในปีนี้

In closing, UNODC will continue to support the region to address urgent issues and challenges, importantly strengthening global digital cooperation to ensure trust, security, and stability in cyberspace in line with the Secretary General's Roadmap for Digital Cooperation. And we do this with our PNI partners like TIJ and with the Government of Thailand.

สุดท้ายนี้ สำนักงาน UNODC มุ่งมั่นที่จะดำเนินการเพื่อช่วยเหลือประเทศต่างๆ ในภูมิภาค จัดการกับความท้าทายสำคัญที่กำลังเกิดขึ้น โดยจะพยายามผลักดันให้เกิดความร่วมมือที่เข้มแข็งทางดิจิทัลในระดับสากล เพื่อสร้างความเชื่อมั่น ความมั่นคงปลอดภัย และเสถียรภาพบนโลกออนไลน์ ให้สอดคล้องกับแผนงานด้านความร่วมมือทางดิจิทัลของเลขาธิการแห่งสหประชาชาติ และเราจะร่วมกันทำไปด้วยกันกับสถาบันเครือข่าย UN-PNI อย่าง TIJ และรัฐบาลไทย

Thank you.
ขอบคุณครับ